IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

DAN HEARON, GERI SHERWOOD, and KYLIN SMITH, on behalf of themselves and all others similarly situated,	
Plaintiffs	**Civil Action No: 3:24-cv-00818**
v.	**JURY TRIAL DEMANDED**
AT&T, INC.	
Defendant	

CLASS ACTION COMPLAINT

Plaintiffs, Dan Hearon, Geri Sherwood, Kylin Smith (hereinafter, "Plaintiffs"), on behalf of themselves and all others similarly situated, for their causes of action against Defendant, AT&T Inc. ("Defendant" or "AT&T"), allege upon personal knowledge as to their own actions, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. This action arises out of Defendant's unauthorized disclosure of the confidential personal information, Personally Identifying Information[1] ("PII" or "Private Information") of Plaintiffs and the proposed Class Members, approximately 73 million current and former customers of AT&T, in a cyberattack on AT&T's systems, announced by AT&T on or around

[1] The Federal Trade Commission defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 17 C.F.R. § 248.201(b)(8).

March 30, 2024.[2] AT&T confirmed that the Private Information of its current and former customers was released on the Dark Web, including but not limited to: full names, email addresses, mailing addresses, phone number, Social Security numbers, dates of birth, AT&T account numbers, and passcodes (the "Data Breach").[3]

2. AT&T, headquartered in Dallas, Texas, is an American multinational telecommunications company providing cellular, broadband internet, and related services.

3. In connection with performing these services, AT&T collects massive amounts of PII from its customers, including Plaintiffs and the Class Members.

4. On information and belief, AT&T failed to undertake adequate measures to safeguard the PII of Plaintiffs and the proposed Class Members, including failing to implement industry standards for data security, and failing to properly train employees on cybersecurity protocols, resulting in the Data Breach.

5. According to AT&T's March 30, 2024, announcement, the "data set" containing Plaintiffs' and Class Members' PII was released on the Dark Web two weeks prior. Whether the data set came from AT&T or one of its vendors was unknown, according to AT&T.

6. As a direct and proximate result of Defendant's failures to protect Plaintiffs' and

---

[2] *AT&T Addresses Recent Data Set Released on the Dark Web,* March 30, 2024 https://about.att.com/story/2024/addressing-data-set-released-on-dark-web.html (last accessed Apr. 2, 2024).

[3] *See also*, Sample Data Breach Notice Letter sent via email to customers **(Exhibit A),** available at https://message.att-mail.com/pub/sf/FormLink?_ri_=X0Gzc2X%3DAQpglLjHJlDQGXDFNmzfjU9O4XzfjfiAvSUjsRzfEtjSgbzg3Bf8sLIgvHGnr88zazczb0zgjXzb2zaAqDWP28KfVXMtX%3DAQpglLjHJlDQGXDFNmzfjU9O4XzfjfiAvSUjgzfzgRa0YRII7YNzesG7zd77c3BrcLzaOzezbI9BXeA4LsIqHPO&_ei_=ET24IA9AB62XJbwCmz6tUrdSfmoQY0S-VhgyPxayyOm5ZThE3gI42qhMSrCXWq2x6AQqeNZoMpg3ZIXn30TAIb5v6m426_y6hxMbZPQiDPOxt-ob.&_di_=2nq23ikl2gfu1bm04079plrl9305fe8078ogcks19cv3m21rkc60 (last accessed Apr. 2, 2024).

the Class Members' sensitive PII and warn them promptly and fully about the Data Breach, Plaintiffs and the proposed Class have suffered widespread injury and damages necessitating Plaintiffs seeking relief on a class wide basis.

PARTIES

7. Plaintiff Dan Hearon is a resident and citizen of Indiana, where he intends to remain. Plaintiff Hearon is a current customer of AT&T. On or around March 31, 2024, Plaintiff Hearon received an email notification from Defendant AT&T notifying him that his Private Information was compromised in the Data Breach.

8. Plaintiff Geri Sherwood is a resident and citizen of Indiana, where she intends to remain. Plaintiff Sherwood is a current customer of AT&T. On or around March 30, 2024, Plaintiff Hearon received an email notification from Defendant AT&T notifying her that her Private Information was compromised in the Data Breach.

9. Plaintiff Kylin Smith is a resident and citizen of Tennessee, where he intends to remain. Plaintiff Smith is a former customer of AT&T. On or around March 30, 2024, Plaintiff Smith received an email notification from Defendant AT&T notifying him that his Private Information was compromised in the Data Breach.

10. Defendant AT&T is a Delaware corporation headquartered in Dallas, Texas, with its principal place of business located at 208 South Akard Street, Dallas, Texas, 75202. Defendant is a citizen of Texas. The registered agent for service of process is CT Corporation System, 1999 Bryan St., Suite 900, Dallas, Texas 75201.

JURISDICTION AND VENUE

11. This Court has personal jurisdiction over Defendant because, personally or through its agents, Defendant operates, conducts, engages in, or carries on a business in this state; it

maintains its principal places of business and headquarters in the Dallas Division of the Northern District of Texas; and committed tortious acts in Texas.

12. This Court has subject matter jurisdiction under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than one hundred (100) members in the proposed Class, and at least one member of the class is a citizen of a state different from Defendant.

13. The Court has supplemental jurisdiction over Plaintiffs' claims arising under state law under 28 U.S.C. § 1367.

14. Venue is proper under 28 U.S.C. § 1391(b)(1) and (2) because Defendant resides in the Dallas Division of the Northern District of Texas and a substantial part of the events and omissions giving rise to Plaintiffs' claims occurred in this district.

FACTUAL BACKGROUND

A. Defendant AT&T

15. Incorporated in 1983, AT&T is an American multinational telecommunications ("telecom") holding company and digital entertainment services company. AT&T is currently the number one telecom company in the United States. In 2023, AT&T's annual revenue was $122 billion.[4]

16. AT&T's services include wireless communications, data/broadband and Internet services, digital video services, local and long-distance telephone services, telecommunications equipment, managed networking, and wholesale services.[5] [6]

17. To provide these services, AT&T requires that its customers provide their PII to

[4] https://www.investopedia.com/markets/quote?tvwidgetsymbol=T (last acc. Apr. 2, 2024).
[5] *Id.*
[6] These services may be collectively referred to as "telecom" services throughout this Complaint.

Defendant, including their names, email addresses, mailing addresses, phone number, Social Security numbers, and dates of birth.

18. In exchange for this information, AT&T promises to safeguard its customers' PII, and to only use this confidential information for authorized purposes.

19. Defendant acknowledges the importance of properly safeguarding the private data and PII of individuals, stating in the Data Breach Notice (**Ex. A**, Sample Notice), that "[w]e take cybersecurity very seriously and privacy is a fundamental commitment at AT&T."[7]

20. Plaintiffs and the proposed Class Members are current and former customers of AT&T and would not have entrusted their PII to Defendant had they known AT&T would not adequately safeguard that information.

21. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and the proposed Class Members' PII, Defendant assumed legal and equitable duties to Plaintiffs, and the members of the Proposed Class, and knew or should have known that they were responsible for protecting their PII from unauthorized disclosure.

22. At all times Plaintiffs and the members of the Proposed Class have taken reasonable steps to maintain the confidentiality of their PII; and, Plaintiffs and the proposed Class Members, relied on Defendant to keep their PII confidential and securely maintained.

B. AT&T Fails to Adequately Safeguard PII—the Data Breach

23. Plaintiffs and the proposed Class Members are current and former customers of AT&T whose personal information, PII, was entrusted to AT&T, in connection with its telecom services.

24. AT&T collected and maintained this PII in its computer information technology

[7] *See* Sample Notice, **Exhibit A.**

systems and networks.

25. On information and belief, on an unknown date, AT&T's systems network was unauthorizedly accessed by an unknown cybercriminal during an external system breach hacking attack, resulting in its customers' PII being compromised and disclosed on the Dark Web. Plaintiffs' and the proposed Class Members' PII that was stored therein included their names, email addresses, mailing addresses, phone number, Social Security numbers, dates of birth, AT&T account numbers, and passcodes—the Data Breach.

26. According to the statement posted by AT&T on its website on March 30, 2024:

> [AT&T] has determined that AT&T data-specific fields were contained in a data set released on the dark web approximately two weeks ago. While AT&T has made this determination, it is not yet known whether the data in those fields originated from AT&T or one of its vendors. With respect to the balance of the data set, which includes personal information such as social security numbers, the source of the data is still being assessed.
>
> AT&T has launched a robust investigation supported by internal and external cybersecurity experts. Based on our preliminary analysis, the data set appears to be from 2019 or earlier, impacting approximately 7.6 million current AT&T account holders and approximately 65.4 million former account holders.
>
> Currently, AT&T does not have evidence of unauthorized access to its systems resulting in exfiltration of the data set. The company is communicating proactively with those impacted and will be offering credit monitoring at our expense where applicable. We encourage current and former customers with questions to visit www.att.com/accountsafety for more information.
>
> As of today, this incident has not had a material impact on AT&T's operations.[8]

27. Even though customers' PII has long been compromised and has since been posted on the Dark Web, AT&T still does not know how that information was accessed.

[8] *AT&T Addresses Recent Data Set Released on the Dark Web,* March 30, 2024 https://about.att.com/story/2024/addressing-data-set-released-on-dark-web.html (last accessed Apr. 2, 2024) ("Website Notice") (copy attached as **Exhibit B**).

28. Defendant's Data Breach Notice (Ex. A) and Website Notice failed to explain *when* the cyberattack occurred, the nature of the cyberattack, or how the cyberattack was perpetrated (i.e., an external system breach (hacking) attack), obfuscating the nature of the Data Breach.[9]

29. AT&T's Data Breach Notice admitted that affected consumers' PII, including their names, email addresses, mailing addresses, phone number, Social Security numbers, dates of birth, AT&T account numbers, and passcodes were compromised in the Data Breach. [10]

30. The Data Breach Notice was careful to qualify, that the "compromised data appears to be from 2019 or earlier and does not contain personal financial information or call history," downplaying the severity and consequences of the Data Breach, but encouraged affected victims to "remain vigilant by monitoring account activity and credit reports" and advising affected victims to sign up for free fraud alerts from nationwide credit bureaus. *Id.*

31. Defendant did not have adequate security protocols to prevent, detect, and stop the cybercriminals from executing the cyberattack on AT&T's systems and accessing the voluminous PII of Plaintiffs and the proposed Class Members in the Data Breach.

32. Further, AT&T failed to adequately train its employees on reasonable cybersecurity protocols and failed to implement reasonable security measures, causing it to lose control over individuals' PII in the Data Breach.

33. Defendant's tortious conduct and breach of contractual obligations, as explained hereinafter, are evidenced by its failure to recognize the Data Breach until cybercriminals had already accessed the data, meaning AT&T had no effective means to detect and prevent attempted data breaches.

[9] Ex. A.
[10] *See Id.*

34. As a result of AT&T's Data Breach, its victims face a lifetime risk of identity theft, as it includes sensitive information that cannot be changed, like their Social Security numbers. Accordingly, AT&T's offer of free credit monitoring is wholly insufficient to compensate Plaintiffs and the Class Members for their damages caused by the Data Breach.

35. Indeed, as a result of the Data Breach which Defendant permitted to occur by virtue of its inadequate data security practices, Plaintiffs and the proposed Class Members have suffered injury and damages, as set forth herein.

C. Plaintiffs' Experiences

i. Plaintiff Hearon

36. Plaintiff Hearon entrusted his PII to AT&T in connection with receiving telecom and internet services.

37. Plaintiff Hearon received AT&T's Data Breach Notice on or around March 30, 2024, informing him that his PII was compromised in the Data Breach.

38. As a direct result of the Data Breach, Plaintiff Hearon has suffered or will imminently suffer injury from the unauthorized disclosure and misuse of his PII that can be directly traced to Defendant.

39. Plaintiff Hearon's PII unauthorizedly disclosed in the Data Breach is now in the possession of cybercriminals and/or on the Dark Web where it can be sold and utilized for fraudulent and criminal purposes.

40. Plaintiff Hearon has spent uncompensated time mitigating the effects of the Data Breach by researching the Data Breach, waiting on the phone with AT&T to inquire about the breach, and freezing his credit. Plaintiff Hearon spent roughly 4-5 hours doing so.

41. In addition, Plaintiff Hearon must now spend additional time and effort attempting

to remediate the harmful effects of the Data Breach, including monitoring his credit reports, and fears for his personal financial security and uncertainty over the information compromised in the Data Breach. He is experiencing feelings of anxiety, sleep disruption, stress, and fear because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that is contemplated and addressed by law.

42. Plaintiff Hearon was highly disturbed by the Data Breach's nature and the thought of cybercriminals accessing his highly sensitive PII and the harm caused by the Data Breach.

43. As a result of AT&T's Data Breach, Plaintiff Hearon faces a lifetime risk of additional identity theft.

ii. Plaintiff Sherwood

44. Plaintiff Sherwood entrusted her PII to AT&T in connection with receiving telecom and internet services.

45. Plaintiff Sherwood received AT&T's Data Breach Notice on or around March 31, 2024, informing her that her PII was compromised in the Data Breach.

46. As a direct result of the Data Breach, Plaintiff Sherwood has suffered or will imminently suffer injury from the unauthorized disclosure and misuse of her PII that can be directly traced to Defendant.

47. Plaintiff Sherwood's PII unauthorizedly disclosed in the Data Breach is now in the possession of cybercriminals and/or on the Dark Web where it can be sold and utilized for fraudulent and criminal purposes.

48. Plaintiff Sherwood has spent uncompensated time mitigating the effects of the Data Breach by checking bank statements and cancelling bank cards. Plaintiff Sherwood spent roughly 2 hours doing so.

49. In addition, Plaintiff Sherwood must now spend additional time and effort attempting to remediate the harmful effects of the Data Breach, including monitoring her credit reports, and fears for her personal financial security and uncertainty over the information compromised in the Data Breach. She is experiencing feelings of anxiety, sleep disruption, stress, and fear because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that is contemplated and addressed by law.

50. Plaintiff Sherwood was highly disturbed by the Data Breach's nature and the thought of cybercriminals accessing her highly sensitive PII and the harm caused by the Data Breach.

51. As a result of AT&T's Data Breach, Plaintiff Sherwood faces a lifetime risk of additional identity theft.

iii. Plaintiff Smith

52. Plaintiff Smith entrusted his PII to AT&T in connection with receiving telecom and internet services.

53. Plaintiff Smith received AT&T's Data Breach Notice on or around March 30, 2024, informing him that his PII was compromised in the Data Breach.

54. As a direct result of the Data Breach, Plaintiff Smith has suffered or will imminently suffer injury from the unauthorized disclosure and misuse of his PII that can be directly traced to Defendant.

55. Plaintiff Smith's PII unauthorizedly disclosed in the Data Breach is now in the possession of cybercriminals and/or on the Dark Web where it can be sold and utilized for fraudulent and criminal purposes.

56. Plaintiff Smith has spent uncompensated time mitigating the effects of the Data Breach by researching the Data Breach and changing all passwords associated with AT&T and other passwords. Plaintiff Smith spent roughly 12 hours doing so.

57. In addition, Plaintiff Smith must now spend additional time and effort attempting to remediate the harmful effects of the Data Breach, including monitoring his credit reports, and fears for his personal financial security and uncertainty over the information compromised in the Data Breach. He is experiencing feelings of anxiety, sleep disruption, stress, and fear because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that is contemplated and addressed by law.

58. Plaintiff Smith was highly disturbed by the Data Breach's nature and the thought of cybercriminals accessing his highly sensitive PII and the harm caused by the Data Breach.

59. As a result of AT&T's Data Breach, Plaintiff Smith faces a lifetime risk of additional identity theft.

D. This Data Breach was Foreseeable by AT&T.

60. Plaintiffs' and the proposed Class Members' PII was provided to AT&T with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access. By failing to do so, Defendant put all Class Members at risk of identity theft, financial fraud, and other harms.

61. Defendant tortiously failed to take the necessary precautions required to safeguard and protect the PII of Plaintiffs and the Class Members from unauthorized disclosure. Defendant's actions represent a flagrant disregard of Plaintiffs' and the other Class Members' rights.

62. Plaintiffs and Class Members were the foreseeable and probable victims of

Defendant's inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing PII and the critical importance of providing adequate security for that information.

63. Cyber-attacks against companies such as Defendant are targeted and frequent. Indeed, according to UpGuard, "[c]ybercriminals know that tech companies often have weaker data protection and overall cybersecurity measures than highly-regulated industries, like healthcare and finance. Instead of targeting these organizations directly for their valuable data, they focus their efforts on the poor data security often found in the first link of the supply chain – tech vendors that store and manage significant amounts of data from these industries."[11]

64. According to the Identity Theft Resource Center's January 24, 2022 report for 2021, "the overall number of data compromises (1,862) is up more than 68 percent compared to 2020. The new record number of data compromises is 23 percent over the previous all-time high (1,506) set in 2017. The number of data events that involved sensitive information (Ex: Social Security numbers) increased slightly compared to 2020 (83 percent vs. 80 percent)."[12]

65. The increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including AT&T. According to IBM's 2022 report, "[f]or 83% of companies, it's not if a data breach will happen, but when."[13]

66. Based on data from the Maine Attorney General, as of August 2022, "…at least 79

[11] UpGuard, Catherine Chipeta, "5 Ways Tech Companies Can Prevent Data Breaches," updated Mar. 2, 2023 available at https://www.upguard.com/blog/how-tech-companies-can-prevent-data-breaches (last acc. Jun. 15, 2023).
[12] *See* "Identity Theft Resource Center's 2021 Annual Data Breach Report Sets New Record for Number of Compromises," Jan. 24, 2022, available at https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/ (last acc. Sept. 26,, 2023Sept. 26, 2023).
[13] IBM, "Cost of a data breach 2022: A million-dollar race to detect and respond," available at https://www.ibm.com/reports/data-breach (last acc. Sept. 26, 2023).

financial service companies have reported data breaches affecting 1,000 or more consumers, and the total number of consumers affected by these breaches could be as high as 9.4 million."[14]

67. PII is of great value to hackers and cybercriminals, and the data compromised in the Data Breach can be used for a variety of unlawful and nefarious purposes, including ransomware and fraudulent misuse, and sale on the Dark Web.

68. PII can be used to distinguish, identify, or trace an individual's identity, such as their name, Social Security number, and financial records. This can be accomplished alone, or in combination with other personal or identifying information that is connected, or linked to an individual, such as their birthdate, birthplace, and mother's maiden name.

69. Given the nature of the Data Breach, it was foreseeable that the compromised PII could be used by hackers and cybercriminals in a variety of different injurious ways. Indeed, the cybercriminals who possess Plaintiffs' and the Class Members' PII can easily obtain their tax returns or open fraudulent credit card accounts in the Class Members' names.

E. AT&T Failed to Comply with FTC Guidelines

70. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

71. In 2016, the FTC updated its publication, *Protecting PII: A Guide for Business*, which establishes cyber-security guidelines for businesses. The guidelines note that businesses

[14] Carter Pape, "Breach data from Maine shows scope of bank, credit union exposures," American Banker, August 24, 2022, available at https://www.americanbanker.com/news/breach-data-from-maine-shows-scope-of-bank-credit-union-exposures

should protect the personal customer information that they keep; properly dispose of PII that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[15]

72. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[16]

73. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

74. These FTC enforcement actions include actions against entities failing to safeguard PII such as Defendant. *See, e.g., In the Matter of LabMD, Inc., A Corp*, 2016-2 Trade Cas. (CCH)

[15] *See* Federal Trade Commission, October 2016, "Protecting Private information: A Guide for Business," available at https://www.bulkorder.ftc.gov/system/files/publications/2_9-00006_716a_protectingpersinfo-508.pdf (last acc. Sept. 26, 2023).
[16] *See id*.

¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

75. AT&T failed to properly implement basic data security practices widely known throughout the industry. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to customer PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

76. Defendant was at all times fully aware of its obligations to protect the PII of Plaintiffs and the Class Members. AT&T was also aware of the significant repercussions that would result from its failure to do so.

F. AT&T Fails to Comply with Industry Standards

77. A number of industry and national best practices have been published and are widely used as a go-to resource when developing an institution's cybersecurity standards.

78. The Center for Internet Security's (CIS) CIS Critical Security Controls (CSC) recommends certain best practices to adequately secure data and prevent cybersecurity attacks, including 18 Critical Security Controls of Inventory and Control of Enterprise Assets, Inventory and Control of Software Assets, Data Protection, Secure Configuration of Enterprise Assets and Software, Account Management, Access Control Management, Continuous Vulnerability Management, Audit Log Management, Email and Web Browser Protections, Malware Defenses, Data Recovery, Network Infrastructure Management, Network Monitoring and Defense, Security Awareness and Skills Training, Service Provider Management, Application Software Security,

Incident Response Management, and Penetration Testing.[17]

79. In addition, the National Institute of Standards and Technology (NIST) recommends certain practices to safeguard systems, *infra,* such as:

a. Control who logs on to your network and uses your computers and other devices.

b. Use security software to protect data.

c. Encrypt sensitive data, at rest and in transit.

d. Conduct regular backups of data.

e. Update security software regularly, automating those updates if possible.

f. Have formal policies for safely disposing of electronic files and old devices.

g. Train everyone who uses your computers, devices, and network about cybersecurity. You can help employees understand their personal risk in addition to their crucial role in the workplace.[18]

80. Further still, the Cybersecurity & Infrastructure Security Agency makes specific recommendations to organizations to guard against cybersecurity attacks, including (1) reducing the likelihood of a damaging cyber intrusion by validating that "remote access to the organization's network and privileged or administrative access requires multi-factor authentication, [e]nsur[ing] that software is up to date, prioritizing updates that address known exploited vulnerabilities identified by CISA[,] [c]onfirm[ing] that the organization's IT personnel have disabled all ports and protocols that are not essential for business purposes," and other steps;

[17] *See* Rapid7, "CIS Top 18 Critical Security Controls Solutions," available at https://www.rapid7.com/solutions/compliance/critical-controls/ (last acc. Sept. 26, 2023).
[18] Federal Trade Commission, "Understanding The NIST Cybersecurity Framework," https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/nist-framework (last acc. Sept. 26, 2023).

(2) taking steps to quickly detect a potential intrusion, including "[e]nsur[ing] that cybersecurity/IT personnel are focused on identifying and quickly assessing any unexpected or unusual network behavior [and] [e]nabl[ing] logging in order to better investigate issues or events[;] [c]onfirm[ing] that the organization's entire network is protected by antivirus/antimalware software and that signatures in these tools are updated," and (3) "[e]nsur[ing] that the organization is prepared to respond if an intrusion occurs," and other steps.[19]

81. Upon information and belief, AT&T failed to implement industry-standard cybersecurity measures, including failing to meet the minimum standards of one or more of NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2) and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established frameworks for reasonable cybersecurity readiness, as well as failing to comply with other industry standards for protecting Plaintiffs' and the proposed Class Members' PII, resulting in the Data Breach.

G. The Data Breach Caused Plaintiffs and the Class Members Injury and Damages

82. Plaintiffs and members of the proposed Class have suffered injury and damages from the exfiltration and misuse of their PII that can be directly traced to AT&T, that has occurred, is ongoing, and/or imminently will occur.

83. As stated prior, in the Data Breach, unauthorized cybercriminals were able to access and acquire the Plaintiffs' and the proposed Class Members' PII, which is now available to be

[19] Cybersecurity & Infrastructure Security Agency, "Shields Up: Guidance for Organizations," available at https://www.cisa.gov/shields-guidance-organizations (last acc. Sept. 26, 2023).

imminently used for fraudulent purposes or has been sold for such purposes, causing widespread injury and damages.

84. The ramifications of AT&T's failure to keep Plaintiffs' and the Class's PII secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security number, driver's license number, date of birth, or other information, such as addresses, without permission, to commit fraud or other crimes.

85. Because AT&T failed to prevent the Data Breach, Plaintiffs and the proposed Class Members have suffered, will imminently suffer, and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. Plaintiffs and the Class Members have suffered, will imminently suffer, or are at an increased risk of suffering:

a. Fraudulent misuse of PII;

b. The loss of the opportunity to control how PII is used;

c. The diminution in value of their PII;

d. The compromise and continuing publication of their PII;

e. Out-of-pocket expenses associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

f. Lost opportunity costs and lost wages associated with the time and effort expended addressing and trying to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

g. Delay in receipt of tax refund monies;

h. Increase in spam texts and telephone calls;

i. Unauthorized use of stolen PII; and

j. The continued risk to their PII, which remains in the possession of AT&T and is subject to further breaches so long as AT&T fails to undertake the appropriate measures to protect the PII in its possession.

86. Furthermore, the Data Breach has placed Plaintiffs and the proposed Class Members at an increased risk of fraud and identity theft.

87. There are myriad dangers which affect victims of identity theft, including: cybercriminals opening new financial accounts, credit cards, and loans in victim's names; victim's losing health care benefits (medical identity theft); hackers taking over email and other accounts; time and effort to repair credit scores; losing home due to mortgage and deed fraud; theft of tax refunds; hackers posting embarrassing posts on victim's social media accounts; victims spending large amounts of time and money to recover their identities; experiencing psychological harm and emotional distress; victims becoming further victimized by repeat instances of identity theft and fraud; cybercriminals committing crimes in victim's names; victims' personal data circulating the Dark Web forever; victims receiving increased spam telephone calls and emails; victims' children or elderly parents having their identities stolen.[20]

88. The FTC recommends that identity theft victims take time and effort intensive or costly steps to protect their personal and financial information after a data breach, including contacting the company where the fraud occurred and asking them to close or freeze accounts and changing login information; contacting one of the credit bureaus to place a fraud alert on

[20] *See* Gaetano DiNardi, Aura.com, "How Bad Is Identity Theft? Is It Serious?" (December 14, 2022) available at https://www.aura.com/learn/dangers-of-identity-theft#:~:text=Fraudsters%20can%20open%20new%20accounts,to%20repair%20your%20credit%20score (last acc. Sept. 26, 2023).

credit files (consider an extended fraud alert that lasts for 7 years if someone steals their identity); reviewing their credit reports; seeking a credit freeze; correcting their credit reports; and other steps such as contacting law enforcement and reporting the identity theft to the FTC.[21]

89. Identity thieves use stolen PII such as Social Security numbers for a variety of crimes, including credit card fraud—just as occurred here—phone or utilities fraud, and bank/finance fraud.

90. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information.

91. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive other services in the victim's name, and may even give the victim's PII to police during an arrest—resulting in an arrest warrant being issued in the victim's name. That can be even more problematic and difficult to remedy for someone who already has a criminal record.

92. Further, according to the Identity Theft Resource Center's 2021 Consumer Aftermath Report, identity theft victims suffer "staggering" emotional tolls: For example, nearly 30% of victims have been the victim of a previous identity crime; an all-time high number of victims say they have contemplated suicide. 35% reported not having enough money to pay for food and utilities, while 14% were evicted because they couldn't pay rent or their mortgage. 54%

[21] *See* Federal Trade Commission, available at https://www.identitytheft.gov/Steps (last acc. Sept. 26, 2023).

percent reported feelings of being violated.[22]

93. What's more, theft of PII is also gravely serious outside of the traditional risks of identity theft. In the last two decades, as more and more of our lives become interconnected through the lens of massively complex cloud computing, PII is valuable property.[23]

94. The value of sensitive information is axiomatic; one need only consider the value of Big Data in corporate America, or that the consequences of cyber theft include heavy prison sentences. Even the obvious risk to reward analysis of cybercrime illustrates beyond doubt that PII has considerable market value.

95. It must also be noted there may be a substantial time lag–measured in years–between when harm occurs versus when it is discovered, and also between when PII and/or financial information is stolen and when it is used.

96. PII are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

97. Where the most PII belonging to Plaintiffs and Class Members was accessible from AT&T's network, there is a strong probability that entire batches of stolen information have been dumped on the black market, and are yet to be dumped on the black market, meaning Plaintiffs and the Class Members are at an increased risk of fraud and identity theft for many years into the

[22] Jason Steele, *Credit Card and ID Theft Statistics*, CreditCards.com (June 11, 2021), avail. at https://www.creditcards.com/statistics/credit-card-security-id-theft-fraud-statistics-1276/ citing Identity Theft Resource Center, "2021 Consumer Aftermath Report," May 26, 2021 available at https://www.idtheftcenter.org/post/the-identity-theft-resource-centers-2021-consumer-aftermath-report-reveals-impacts-on-covid-19-identity-crime-victims/ (last acc. Sept. 26, 2023).

[23] *See, e.g.*, John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("Private information") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("Private information, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

future. Thus, Plaintiffs and the Class Members must vigilantly monitor their financial accounts for many years to come.

98. Social Security numbers are among the worst kind of PII to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud.[24]

99. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[25] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

100. Moreover, it is not an easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number,

[24] *See* U.S. Social Security Administration, "Identity Theft and Your Social Security Number," Publication No. 05-10064, July 2021, available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last acc. Feb. 25, 2023)
[25] *See id.*

so all of that old bad information is quickly inherited into the new Social Security number."[26]

101. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[27] ...Accordingly, the Data Breach has caused Plaintiffs and the proposed Class Members a greatly increased risk of identity theft and fraud, in addition to the other injuries and damages set forth herein, specifically the unauthorized disclosure, lost time and efforts in remediating the impact of the Data Breach, and other injury and damages as set forth in the preceding paragraphs.

102. Another example of criminals using PII for profit is the development of "Fullz" packages.[28]

103. Cyber-criminals can cross-reference two sources of PII to marry unregulated data

---

[26] *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR, Brian Naylor, Feb. 9, 2015, http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited September 1, 2021).

[27] *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, Tim Greene, Feb. 6, 2015, http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Sept. 27, 2023).

[28] "Fullz" is fraudster-speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record or more on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz", which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.*, Brian Krebs, *Medical Records For Sale in Underground Stolen From Texas Life Insurance Firm*, KREBS ON SECURITY, (Sep. 18, 2014) https://krebsonsecurity.com/tag/fullz/.

available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as Fullz packages.

104. The development of Fullz packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and other members of the proposed Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

105. AT&T knew or should have known of these harms which would be caused by the Data Breach it permitted to occur, and strengthened its data systems accordingly.

CLASS ALLEGATIONS

114. Plaintiffs incorporate by reference all other paragraphs of this Complaint as if fully set forth herein.

115. Plaintiffs bring this nationwide class action individually and on behalf of all other persons similarly situated pursuant to Rule 23(a) of the Federal Rules of Civil Procedure, and Fed. R. Civ. P. 23(b)(3).

116. Plaintiffs propose the following Class definition (“Nationwide Class” or “Class”), subject to amendment based on information obtained through discovery:

All persons whose PII was compromised as a result of the Data Breach announced by AT&T on or about March 30, 2024, including all persons who received Defendant's Data Breach Notice.

117. Excluded from the Class are Defendant's members, officers, directors, and employees; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families, and members of their staff.

118. Plaintiffs reserve the right to amend the definition of the Class or add a class or subclass if further information and discovery indicate that the definition of the Class should be narrowed, expanded, or otherwise modified.

119. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of Class Members' claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims for each Class Member.

120. This action satisfies the requirements for a class action under Fed. R. Civ. P. 23(a)(1)-(3) and Fed. R. Civ. P. 23(b)(2), including requirements of numerosity, commonality, typicality, adequacy, predominance, and superiority.

121. **Numerosity, Fed. R. Civ. P. 23(a)(1):** The members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, based on information and belief, the PII of approximately 73 million individuals was compromised in the Data Breach. Such information is readily ascertainable from Defendant's records.

122. **Commonality, Fed. R. Civ. Proc. 23(a)(2), and Predominance, Fed. R. Civ.**

Proc. 23(b)(3): There are numerous questions of law and fact common to the Class. As such, there is a well-defined community of interest among the Members of the Class. These questions predominate over questions that may affect only individual Class Members because AT&T has acted on grounds generally applicable to the Class. Such common legal or factual questions include, but are not limited to:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' PII;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

d. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations including, *e.g.*, the FTC Act;

e. Whether computer hackers obtained Plaintiffs' and Class Members' PII in the Data Breach;

f. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

g. Whether Defendant failed to adequately respond to the Data Breach, including failing to timely notify the Plaintiffs and the Class Members;

h. Whether Defendant's failures amounted to negligence;

i. Whether Defendant breached its contractual promises;

j. Whether Defendant was unjustly enriched;

k. Whether Defendant intruded into the private affairs of Plaintiffs and the Class Members;

l. Whether Plaintiffs and the Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

m. Whether Defendant's acts violated the law, including the state consumer and privacy protection laws alleged herein; and

n. Whether Plaintiffs and the Class Members are entitled to damages including compensatory and punitive damages, and/or injunctive relief.

123. **Typicality, Fed. R. Civ. P. 23(a)(3):** The claims or defenses of Plaintiffs are typical of the claims or defenses of the proposed Class because Plaintiffs' claims are based upon the same legal theories and same violations of law. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' PII, like that of every other Class Member, was compromised in the Data Breach, and all arise from the same set of facts regarding AT&T's failures:

a. to protect Plaintiffs' and Class Members' PII;

b. to discover and remediate the security breach of its computer systems more quickly; and

c. to disclose to Plaintiffs and Class Members in a complete and timely manner information concerning the security breach and the theft of their Private Information.

124. **Adequacy, Fed. R. Civ. P. 23(a)(4):** Plaintiffs will fairly and adequately represent and protect the interests of the members of the Class. Plaintiffs' Counsel are competent and experienced in litigating class actions.

125. **Superiority, Fed. R. Civ. P. 23(b)(3):** A class action is a superior method for the fair and efficient adjudication of this controversy because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy, and joinder of the Class Members is otherwise impracticable. Class treatment presents a superior mechanism for fairly resolving similar issues and claims without repetitious and wasteful litigation for many reasons, including the following:

a. It would be a substantial hardship for most individual members of the Class if they were forced to prosecute individual actions. Many members of the Class are not in the position to incur the expense and hardship of retaining their own counsel to prosecute individual actions, which in any event might cause inconsistent results.

b. When the liability of Defendant has been adjudicated, the Court will be able to determine the claims of all members of the Class. This will promote global relief and judicial efficiency in that the liability of Defendant to all Class Members, in terms of money damages due and in terms of equitable relief, can be determined in this single proceeding rather than in multiple, individual proceedings where there will be a risk of inconsistent and varying results.

c. A class action will permit an orderly and expeditious administration of the Class claims, foster economies of time, effort, and expense, and ensure uniformity of decisions. If Class Members are forced to bring individual suits, the transactional costs, including those incurred by Defendant, will increase dramatically, and the courts will be clogged with a multiplicity of

lawsuits concerning the very same subject matter, with identical fact patterns and the same legal issues. A class action will promote a global resolution and will promote uniformity of relief as to the Class Members and as to Defendant.

d. This lawsuit presents no difficulties that would impede its management by the Court as a class action. The class certification issues can be easily determined because the Class includes only AT&T's customers, the legal and factual issues are narrow and easily defined, and the Class membership is limited. The Class does not contain so many persons that would make the Class notice procedures unworkable or overly expensive. The identity of the Class Members can be identified from Defendant's records, such that direct notice to the Class Members would be appropriate.

126. **Injunctive and Declaratory Relief, Fed. R. Civ. Proc. 23(b)(2):** In addition, Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

127. Finally, all members of the proposed Class are readily ascertainable. AT&T has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and the Class)

128. Plaintiffs re-allege and incorporate by reference all paragraphs above as if fully set forth herein.

129. Defendant collected the PII of Plaintiffs and the proposed Class Members and stored this information in its computer information technology systems.

130. Defendant had full knowledge of the sensitivity of the PII to which it was entrusted, and the types of harm that Plaintiffs and the Class Members could and would suffer if the PII was wrongfully disclosed to unauthorized persons. Defendant had a duty to Plaintiffs and each Class Member to exercise reasonable care in holding, safeguarding, and protecting that information.

131. Plaintiffs and the Class Members were the foreseeable victims of any inadequate safety and security practices. Plaintiffs and the Class Members had no ability to protect their data in Defendant's possession.

132. By collecting and storing this data in its computer systems, Defendant had a duty of care to use reasonable means to secure and safeguard it, to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect if that PII was exposed to the internet and to give prompt notice to those affected in the case of a data breach.

133. Defendant owed a common law duty of care to Plaintiffs and the Class Members to provide adequate data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the PII.

134. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

135. Defendant breached its duties, and was negligent, by acts of omission or

commission, by failing to use reasonable measures to protect the Plaintiffs' and Class Members' PII. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiffs' and Class Members' PII;

b. Failing to adequately train employees on proper cybersecurity protocols;

c. Failing to adequately monitor the security of its networks and systems;

d. Failure to periodically ensure that its network system had plans in place to maintain reasonable data security safeguards;

e. Allowing unauthorized access to Plaintiffs' and Class Members' PII;

f. Failing to timely notify Plaintiffs and Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

136. It was foreseeable that Defendant's failure to use reasonable measures to protect Plaintiffs' and Class Members' PII would result in injury to Plaintiffs and Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyber-attacks and data breaches in the industry.

137. It was therefore foreseeable that the failure to adequately safeguard Plaintiffs' and Class Members' PII would result in one or more types of injuries to them.

138. As a direct and proximate result of Defendant's negligence set forth in the preceding paragraphs, Plaintiffs and Class Members have suffered injury and damages as set forth herein, including but not limited to fraudulent misuse of their PII; loss of the opportunity to control how their PII is used; diminution in value of their PII; compromise and continuing publication of their

PII; and are entitled to compensatory, actual, and punitive damages as a result of the Data Breach.

139. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II
NEGLIGENCE PER SE
(On Behalf of Plaintiffs and the Class)

140. Plaintiffs re-allege and incorporate by reference all paragraphs above as if fully set forth herein.

141. Pursuant to Federal Trade Commission, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

142. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant's, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

143. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored, and the foreseeable consequences of the Data Breach for companies of Defendant's magnitude, including, specifically, the immense damages that would result to Plaintiffs and Class Members due to the valuable nature of the Private Information at issue in this

case—including Social Security numbers.

144. Defendant's violations of Section 5 of the FTC Act constitute negligence *per se.*

145. Plaintiff and Class Member are within the class of persons that the FTC Act was intended to protect.

146. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of its failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and members of the Class.

147. Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

148. Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated and "impacted" individuals whose Private Information was accessed during the Data Breach, including: (a) invasion of privacy; (b) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) financial "out of pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) diminution of value of their Private Information; (h) anxiety, annoyance and nuisance, (i) nominal damages, and (j) the future costs of identity theft monitoring.

149. Moreover, Plaintiffs' and Class Members' Private Information remains at risk, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Private Information.

150. Therefore, Plaintiffs and Class Members are also entitled to injunctive relief

requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit and identity theft monitoring to all Class Members.

COUNT III
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Class)

151. Plaintiffs re-allege and incorporate by reference all paragraphs above as if fully set forth herein.

152. Through their course of conduct, Defendant, Plaintiffs, and Class Members entered into implied contracts for Defendant to provide services and that Defendant would deal with them fairly and in good faith, as well as implied contracts for Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiffs' and Class Members' PII entrusted to Defendant.

153. Specifically, Plaintiffs and the Class Members entered into valid and enforceable implied contracts with Defendant when they first applied to receive or received Defendant's services.

154. The valid and enforceable implied contracts that Plaintiffs and Class Members entered into with Defendant included Defendant's promise to protect nonpublic PII given to Defendant, or that Defendant created on its own, from unauthorized disclosures. Plaintiffs and Class Members allowed their PII to be provided in reliance of that promise.

155. Defendant solicited and invited Plaintiffs and Class Members to provide their PII, directly or indirectly, as part of Defendant's regular business practices. Plaintiffs and Class Members accepted Defendant's offers and provided their PII to Defendant.

156. In entering into such implied contracts, Plaintiffs and Class Members reasonably

believed and expected that Defendant's data security practices complied with industry standards and relevant laws and regulations, including the FTC Act.

157. Plaintiffs and Class Members reasonably believed and expected that Defendant would adequately employ adequate data security to protect that PII. Defendant failed to do so.

158. Under the implied contracts, Defendant promised and was obligated to: (a) provide services to Plaintiffs and Class Members; and (b) protect Plaintiffs' and the Class Members' PII: (i) provided to obtain such services and/or (ii) created in connection therewith. In exchange, Plaintiffs and Class Members agreed to pay money for these services and to turn over their PII.

159. Both the provision of these services, and the protection of Plaintiffs' and Class Members' PII, were material aspects of these implied contracts.

160. Plaintiffs and Class Members would not have entrusted their PII to Defendant and entered into these implied contracts with Defendant without an understanding that their PII would be safeguarded and protected; nor would they have entrusted their PII to Defendant, directly or indirectly, in the absence of its implied promise to monitor its computer systems and networks to ensure that PII was not disclosed to unauthorized parties and exposed to the public as occurred in the Data Breach.

161. A meeting of the minds occurred when Plaintiffs and the Class Members agreed to, and did, provide their PII to Defendant and/or paid for services, whether directly or indirectly, for, amongst other things, (a) the provision of such services and (b) the protection of their PII.

162. Plaintiffs and the Class Members performed their obligations under the contracts when they paid for services and/or provided their valuable Private Information to Defendant, directly or indirectly.

163. Defendant materially breached its contractual obligations to protect the nonpublic

PII of Plaintiffs and Class Members which Defendant required and gathered.

164. Under Texas law, good faith is an element of every contract. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form. Evading the spirit of the bargain and abusing the power to specify terms constitute examples of bad faith in the performance of contracts.

165. Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or may consist of inaction, and fair dealing may require more than honesty. Examples of bad faith are evasion of the spirit of the bargain and abuse of a power to specify terms.

166. Defendant materially breached its contractual obligations to deal fairly and in good faith with Plaintiffs and the Class Members when it failed to take adequate precautions to prevent the Data Breach and failed to promptly notify them of the Data Breach.

167. The Data Breach was a reasonably foreseeable consequence of Defendant's conduct, by acts of omission or commission, in breach of these contracts.

168. As a result of Defendant's failure to fulfill the data security protections promised in these contracts, Plaintiffs and Class Members did not receive the full benefit of their bargains, and instead received services that were of a diminished value compared to those described in the contracts. Plaintiffs and Class Members were therefore damaged in an amount at least equal to the difference in the value of the services with data security protection they paid for and that which they received.

169. Had Defendant disclosed that its data security was inadequate or that it did not

adhere to industry-standard security measures, neither the Plaintiff, the Class Members, nor any reasonable person would have purchased services from Defendant or entrusted their valuable Private Information to it.

170. As a direct and proximate result of the Data Breach, Plaintiffs and the Class Members have suffered injury and damages as set forth herein and have been irreparably harmed, as well as suffering and the loss of the benefit of the bargain they had struck with Defendant by paying for Defendant's services and/or entrusting their valuable Private Information to Defendant.

171. Plaintiffs and the Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

172. Plaintiffs and the Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT IV
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Class)

173. Plaintiffs re-allege and incorporate by reference all paragraphs above as if fully set forth herein.

174. Plaintiffs bring this claim in the alternate to their claim for Breach of Implied Contract (Count III).

175. Plaintiffs and proposed Class Members conferred benefits upon Defendant in the form of monies received by AT&T, and in the form of valuable PII entrusted to Defendant.

176. Defendant appreciated or knew of these benefits that it received. And under

principles of equity and good conscience, this Court should not allow Defendant to retain the full value of these benefits—specifically, the monies and PII of Plaintiffs and members of the Class.

177. After all, Defendant failed to adequately protect Plaintiffs' and Class Members' PII. And if such inadequacies were known, then Plaintiffs and the members of the Class would never have conferred payment to Defendant, nor permitted the disclosure of their PII to Defendant.

178. As a result of Defendant's wrongful conduct as alleged herein, Defendant has been unjustly enriched at the expense of, and to the detriment of, Plaintiffs and the Class Members.

179. As a direct and proximate result of Defendant's unjust enrichment set forth in the preceding paragraphs, Plaintiffs and Class Members have suffered injury and damages as set forth herein, including but not limited to fraudulent misuse of their PII; loss of the opportunity to control how their PII is used; diminution in value of their PII; and the compromise and continuing publication of their PII and thus are entitled to damages as a result of the Data Breach.

180. Defendant's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein.

181. Under the common law doctrine of unjust enrichment, it is inequitable for Defendant to retain the benefits it received, and is still receiving, without justification, from Plaintiffs and Class Members in an unfair, unconscionable, and oppressive manner. Defendant's retention of such funds under circumstances making it inequitable to do so constitutes unjust enrichment.

182. The financial benefits derived by Defendant rightfully belong to Plaintiffs and Class Members. Defendant should be compelled to disgorge in a common fund for the benefit of Plaintiffs and Class Members all wrongful or inequitable proceeds collected by Defendant. A constructive trust should be imposed upon all wrongful or inequitable sums received by

Defendant traceable to Plaintiffs and Class Members.

183. Plaintiffs and the Class Members have no adequate remedy at law.

COUNT V
INVASION OF PRIVACY—INTRUSION INTO PRIVATE AFFAIRS
(On Behalf of Plaintiffs and the Class)

184. Plaintiffs re-allege and incorporate by reference all paragraphs above as if fully set forth herein.

185. Plaintiffs and the Class Members had a legitimate expectation of privacy to their PII and were entitled to the protection of this information against disclosure to unauthorized third parties.

186. Defendant owed a duty to Plaintiffs and the Class Members to keep their PII confidential.

187. Defendant failed to protect said PII and exposed the PII of Plaintiffs and the Class Members to unauthorized persons in the Data Breach.

188. Defendant allowed unauthorized third parties access to and examination of the PII of Plaintiffs and the Class Members, by way of Defendant's failure to protect the PII.

189. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII of Plaintiffs and the Class Members is highly offensive to a reasonable person.

190. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiffs' and the Class Members' PII was disclosed to Defendant in connection with AT&T's services, but privately with an intention that the PII would be kept confidential and would be protected from unauthorized disclosure. Plaintiffs and the Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

191. The Data Breach constitutes an intentional or reckless interference by Defendant with Plaintiffs' and the Class Members' interests in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

192. Defendant acted with a knowing state of mind when it permitted the Data Breach to occur because it had actual knowledge that its data security practices were inadequate and insufficient.

193. Defendant acted with reckless disregard for Plaintiffs' and Class Members' privacy when it allowed improper access to its systems containing Plaintiffs' and Class Members' PII.

194. Defendant was aware of the potential of a data breach and failed to adequately safeguard its systems and implement appropriate policies to prevent the unauthorized release of Plaintiffs' and Class Members' PII.

195. Because Defendant acted with this knowing state of mind, it had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiffs and the Class Members.

196. As a direct and proximate result of the Defendant's invasion of privacy, the PII of Plaintiffs and the Class Members was disclosed to third parties without authorization, causing Plaintiffs and the Class Members to suffer injury and damages as set forth herein, including but not limited to fraudulent misuse of their PII; loss of the opportunity to control how their PII is used; diminution in value of their PII; and compromise and continuing publication of their PII and, thus, are entitled to damages.

197. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to

future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

198. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class Members in that the PII maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiffs and the Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiffs and the Class Members.

COUNT VI
BAILMENT
(On Behalf of Plaintiffs and the Class)

199. Plaintiffs re-allege and incorporate by reference all paragraphs above as if fully set forth herein.

200. Plaintiffs, the Class Members, and Defendant contemplated a mutual benefit bailment when the Plaintiffs and putative members of the Class transmitted their PII to Defendant solely for the purpose of obtaining telecom services.

201. Plaintiffs and the Class entrusted their PII to Defendant for a specific purpose—to obtain telecom services—with an implied contract that the trust was to be faithfully executed, and the PII was to be accounted for when the special purpose was accomplished.

202. Defendant accepted the Plaintiffs' and the Class's PII for the specific purpose of telecom services.

203. Defendant was duty bound under the law to exercise ordinary care and diligence in safeguarding Plaintiffs' and the Class's PII.

204. Plaintiffs' and the Class's PII was used for a different purpose than Plaintiffs and

the Class intended, for a longer time period and/or in a different manner or place than Plaintiffs and the Class intended.

205. As set forth in the preceding paragraphs, Plaintiffs and the Class Members were damaged thereby.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, Dan Hearon, Geri Sherwood, and Kyrin Smith, on behalf of themselves, and all others similarly situated, pray for judgment as follows:

A. Trial by jury pursuant to Fed. R. Civ. Proc. 38(b) on all claims so triable;

B. An Order certifying this case as a class action on behalf of Plaintiffs and the proposed Class, appointing Plaintiffs as class representative, and appointing their counsel to represent the Class;

C. Awarding Plaintiffs and the Class damages that include applicable compensatory, actual, exemplary, and statutory damages, and punitive damages, as allowed by law;

D. Awarding restitution and damages to Plaintiffs and the Class in an amount to be determined at trial;

E. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiffs and the Class;

F. Awarding injunctive relief as is necessary to protect the interests of Plaintiffs and the Class;

G. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the transmitted PII;

H. Awarding attorneys' fees and costs, as allowed by law;

I. Awarding prejudgment and post-judgment interest, as provided by law;

J. Granting Plaintiffs and the Class leave to amend this complaint to conform to the evidence produced at trial; and,

K. Any and all such relief to which Plaintiffs and the Class are entitled.

Dated: April 4, 2024

Respectfully submitted,

/s/ Joe Kendall

JOE KENDALL
Texas Bar No. 11260700
KENDALL LAW GROUP, PLLC
3811Turtle Creek Blvd., Suite 825
Dallas, Texas 75219
214-744-3000 / 214-744-3015 (Facsimile)
jkendall@kendalllawgroup.com

Lynn A. Toops*
Amina A. Thomas*
COHEN & MALAD, LLP
One Indiana Square, Suite 1400
Indianapolis, Indiana 46204
(317) 636-6481
ltoops@cohenandmalad.com
athomas@cohenandmalad.com

J. Gerard Stranch, IV *
Andrew E. Mize*
Grayson Wells*
STRANCH, JENNINGS & GARVEY, PLLC
The Freedom Center
223 Rosa L. Parks Avenue, Suite 200
Nashville, Tennessee 37203
(615) 254-8801
(615) 255-5419 (facsimile)
gstranch@stranchlaw.com
amize@stranchlaw.com
gwells@stranchlaw.com

* *Pro Hac Vice* Application forthcoming

Counsel for Plaintiffs and the Proposed Class